Homework 1 (Due Mar. 26)

1. The well-known Caesar Cipher is a simple shift cipher based on the following encryption/decryption algorithm.

Let x, y, k $\in Z_{26}$

Encryption: $E_k(x) \equiv y = x+k \bmod 26$

Decryption: $D_k(x) \equiv x= y-k \bmod 26$

Now let us improve this shift cipher by generalizing the encryption function. This cipher encrypts by multiplying the plaintext by one part of the key followed by addition of another part of the key.

Let x, y, a, b $\in Z_{26}$

Encryption: $E_k(x) \equiv y = ax+k \bmod 26$

Decryption: $D_k(x) \equiv x = a^{-1}(y-b) \bmod 26$

With the key k = (a,b) which has the restriction; gcd(a, 26) = 1

Let the key be k=(a,b) = (9,13), and the plaintext be ATTACK = $x_1,x_2,\ldots,x_6$ = 0, 19, 19, 0, 2, 10.

(1) What is its ciphertext?

(2) And show that you can get the same plaintext from this ciphertext by using the decryption algorithm.

(3) Find out the key space. (How many keys are possible?)

2. Consider a Feistel cipher with four rounds and P=(L0, R0). What is the ciphertext C if the round function is

(1) $F(R_{i-1}, K_i) = K_i$

(2) (2) $F(R_{i-1}, K_i) = R_{i-1} \oplus K_i$